UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, DC 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
08/825,102	03/27/97	GOLAN G	0866/0D108

LM21/0301

S. PETER LUDWIG
DARBY & DARBY P.C.
805 THIRD AVENUE
NEW YORK NY 10022

EXAMINER	
NGUYEN, N	
ART UNIT	**PAPER NUMBER**
2787	

DATE MAILED: 03/01/99

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

☆U.S.GOVERNMENT PRINTING OFFICE 1995-319-826

UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office

NOTICE OF ALLOWANCE AND ISSUE FEE DUE

LM21/0301

S. PETER LUDWIG
DARBY & DARBY P.C.
805 THIRD AVENUE
NEW YORK NY 10022

APPLICATION NO.	FILING DATE	TOTAL CLAIMS	EXAMINER AND GROUP ART UNIT		DATE MAILED
08/825,102	03/27/97	019	NGUYEN, N	2787	03/01/99
First Named Applicant: GULAN,		35 USC 154(b) term ext. =		0 Days.	

TITLE OF INVENTION: SECURITY MONITOR

ATTY'S DOCKET NO.	CLASS-SUBCLASS	BATCH NO.	APPLN. TYPE	SMALL ENTITY	FEE DUE	DATE DUE
2 0866/0D108	713-200.000		P71	UTILITY YES	$605.00	06/01/99

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED.

THE ISSUE FEE MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED.

HOW TO RESPOND TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.
If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is changed, pay twice the amount of the FEE DUE shown above and notify the Patent and Trademark Office of the change in status, or
B. If the status is the same, pay the FEE DUE shown above.

If the SMALL ENTITY is shown as NO:

A. Pay FEE DUE shown above, or

B. File verified statement of Small Entity Status before, or with, payment of 1/2 the FEE DUE shown above.

II. Part B-Issue Fee Transmittal should be completed and returned to the Patent and Trademark Office (PTO) with your ISSUE FEE. Even if the ISSUE FEE has already been paid by charge to deposit account, Part B Issue Fee Transmittal should be completed and returned. If you are charging the ISSUE FEE to your deposit account, section "4b" of Part B-Issue Fee Transmittal should be completed and an extra copy of the form should be submitted.

III. All communications regarding this application must give application number and batch number.
Please direct all communications prior to issuance to Box ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

Notice of Allowability

Application No.	Applicant(s)
08/825,102	Gilad Goland
Examiner	**Group Art Unit**
Nguyên X. Nguyên	2787

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance and Issue Fee Due or other appropriate communication will be mailed in due course.

☒ This communication is responsive to *the amendment filed on February 08, 1999*.

☒ The allowed claim(s) is/are *1-19*.

☐ The drawings filed on _____ are acceptable.

☐ Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

☐ All ☐ Some* ☐ None of the CERTIFIED copies of the priority documents have been

☐ received.

☐ received in Application No. (Series Code/Serial Number) _____.

☐ received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

*Certified copies not received: _____.

☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

A SHORTENED STATUTORY PERIOD FOR RESPONSE to comply with the requirements noted below is set to EXPIRE **THREE MONTHS** FROM THE "DATE MAILED" of this Office action. Failure to timely comply will result in ABANDONMENT of this application. Extensions of time may be obtained under the provisions of 37 CFR 1.136(a).

☒ Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL APPLICATION, PTO-152, which discloses that the oath or declaration is deficient. A SUBSTITUTE OATH OR DECLARATION IS REQUIRED.

☐ Applicant MUST submit NEW FORMAL DRAWINGS

☐ because the originally filed drawings were declared by applicant to be informal.

☐ including changes required by the Notice of Draftsperson's Patent Drawing Review, PTO-948, attached hereto or to Paper No. _____.

☐ including changes required by the proposed drawing correction filed on _____, which has been approved by the examiner.

☐ including changes required by the attached Examiner's Amendment/Comment.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the reverse side of the drawings. The drawings should be filed as a separate paper with a transmittal lettter addressed to the Official Draftsperson.

☐ Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Any response to this letter should include, in the upper right hand corner, the APPLICATION NUMBER (SERIES CODE/SERIAL NUMBER). If applicant has received a Notice of Allowance and Issue Fee Due, the ISSUE BATCH NUMBER and DATE of the NOTICE OF ALLOWANCE should also be included.

Attachment(s)

☐ Notice of References Cited, PTO-892

☐ Information Disclosure Statement(s), PTO-1449, Paper No(s). _____

☐ Notice of Draftsperson's Patent Drawing Review, PTO-948

☐ Notice of Informal Patent Application, PTO-152

☒ Interview Summary, PTO-413

☒ Examiner's Amendment/Comment

☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material

☒ Examiner's Statement of Reasons for Allowance

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with attorney Ludwig on February 25, 1999.

2. The application has been amended as follows:

In amended claim 8, line 11, after "flag", --when-- has been added.

In amended claim 10, line 11, "and" has been deleted.

3. The following is an examiner's statement of reasons for allowance:

Independent claims 1, 5, 8-10 and 16 are allowable over the prior art of record because the prior art does not teach or fairly suggest the following:

Regarding claim 1, the prior art fails to teach a method of creating a secure sandbox around both a monitored application and one or more software components associated therewith in accordance with a predetermined security policy, said method comprising the steps of: a) intercepting a selected set of application programming interface (API) function calls issued by said monitored application by replacing the addresses of all API functions to be intercepted in an import data table associated with said monitored application with addresses of security monitor functions, each security monitor function associated with a different API function; b) intercepting

API function calls issued by said software component by replacing the addresses of API functions to be intercepted in an import data table associated with said software component with addresses of stub functions, each stub function operative to call a security monitor function associated with a different API function; c) intercepting non-API function calls issued by said software component by replacing the addresses of non-API functions to be intercepted in an import data table associated with said software component with addresses of stub functions, each stub function operative to call a security monitor function associated with a different non-API function; d) creating a call chain operative to permit distinguishing between function calls made by said software component from function calls made by monitored application; e) blocking intercepted API calls that are forbidden according to the security policy; and f) allowing intercepted API calls that are permitted according to the security policy.

Regarding claim 5, the prior art fails to teach a method of monitoring the execution of an application and one or more software components associated therewith in accordance with a predetermined security policy, said method comprising the steps of: a) intercepting a selected set of application programming interface (API) function calls issued by said monitored application by replacing the addresses of all API functions to be intercepted in an import data table associated with said monitored application with addresses of security monitor functions, each security monitor function associated with a different API function; b) intercepting API function calls issued by said software component by replacing the addresses of API functions to be intercepted in an import data table associated with said software component with addresses of stub functions,

each stub function operative to call a security monitor function associated with a different API function; c) intercepting non-API function calls issued by said software component by replacing the addresses of non-API functions to be intercepted in an import data table associated with said software component with addresses of stub functions, each stub function operative to call a security monitor function associated with a different non-API function; d) determining whether an intercepted API call issued by said monitored application originated from a non-API call issued by the software component via the generation of a call chain by said software component when a non-API function is called; e) blocking intercepted API calls that originated with a non-API call from the software component that are forbidden according to the security policy; and f) allowing intercepted API calls that originated with a non-API call from the software component that are permitted according to the security policy.

Regarding claim 8, the prior art fails to teach a method of monitoring the execution of an application and one or more software components associated therewith in accordance with a predetermined security policy, said method comprising the steps of: a) injecting a security monitor into the address space of said monitored application; b) generating a plurality of stub function corresponding to application programming interface (API) function calls and non-API function calls which are called by the software component; c) redirecting all API calls and all non-API calls made by the software component; d) redirecting API calls made by said monitored application to said security monitor; e) setting a flag when said software component makes a call to either an API function or a non-API function; f) redirecting a portion of API calls received by

said plurality of stub functions to said security monitor; g) redirecting said non-API calls made by the software component to their corresponding non-API functions; and h) applying the predetermined security policy to an API call when said flag is set.

Regarding claim 9, the prior art fails to teach a method of monitoring the execution of an application and one or more software components associated therewith in accordance with a predetermined security policy, said method comprising the steps of: a) applying interception to the application including all its modules whether loaded initially or during execution thereof; b) detecting the loading of a software component external to the application; c) applying interception to all calls made by the software component to functions located in other modules; and d) applying the security policy to said calls made by the software component.

Regarding claim 10, the prior art fails to teach a method of monitoring the execution of an application and one or more software components associated therewith in accordance with a predetermined security policy, said method comprising the steps of: a) installing means for interception within said monitored application including all modules associated therewith whether loaded initially or during execution thereof; b) detecting the loading of a software component external to said monitored application; c) installing means for intercepting all API and non-API function calls made by the software component to functions located in other modules; d) setting a flag when a function call is issued by the software component to any function located in another module located external thereto; and e) applying the security policy to an API call when said flag is set.

Regarding claim 16, the prior art fails to teach a method of creating a secure sandbox around both a monitored application and one or more software components associated therewith in accordance with a predetermined security policy, said method comprising the steps of: a) intercepting a selected set of application programming interface (API) function calls issued by said monitored application by replacing the addresses of all API functions to be intercepted in an import data table associated with said monitored application with addresses of security monitor functions, each security monitor function associated with a different API function; b) detecting a load type API function called issued by said monitored application; c) blocking intercepted API calls that are forbidden according to the security policy; and d) allowing intercepted API calls that are permitted according to the security policy.

4. The remaining claims 2-4, 6, 7, 11-15 and 17-19 are allowed for at least the same reason as set for claims 1, 5, 8-10 and 16.

5. Any comments considered necessary by applicant must be submitted no later than the payment of the Issue Fee and, to avoid processing delays, should preferable accompany the Issue Fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nguyên X. Nguyêñ whose telephone number is (703) 306 9131.

The examiner can normally be reached on Monday-Thursday from 6:30 AM to 4:00 PM, Eastern Time. The examiner can also be reached on alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hassan Kizou, can be reached on (703) 305 4744.

7. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group receptionist whose telephone number is (703) 305-3900.

Any response to this office action should be mailed to :

Commissioner of Patents and Trademarks

Washington, D.C. 20231

or faxed to:

(703) 308-9051, (for formal communications intended for entry)

Hand-delivered responses should be brought to

Crystal Park II, 2121 Crystal Drive

Arlington, Virginia, (Receptionist).

EXAMINER

Nguyên X. Nguyêñ

Art Unit 2787

February 25, 1999

HASSAN KIZOU

PRIMARY EXAMINER